

Listing of Claims:

1. (Currently Amended) A system for securely providing biometric input from a user, comprising:

~~a biometric sensor;~~

a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which ~~it~~ the security component is securely operably connected;

a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

a card reader for repeatedly accessing the stored secrets and stored identifying information, wherein the stored identifying information comprises stored biometric information of the authorized holder and wherein the card reader is configured to repeatedly access the stored secrets and stored identifying information upon beginning a security-sensitive operation and is configured to terminate repeatedly accessing upon completion of the security-sensitive operation;

means for operably inserting the card into the card reader; ~~and~~

means for ~~securely operably connecting~~ establishing a secure, operable connection between the biometric sensor, the card reader, and the security component;

means for comparing the repeatedly obtained biometric information to the stored biometric information of the authorized holder of the card; and

means for concluding, within the security component, that the security-sensitive operation is authentic based on all the one or more other components which are securely operably connected to the security component remaining securely operably connected to the security component until completion of the security-sensitive operation.

Claim 2 (Canceled).

3. (Original) The system according to Claim 1, wherein selected ones of the secure

operable connections are made using one or more buses of the security component.

4. (Original) The system according to Claim 1, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

5. (Original) The system according to Claim 4, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

6. (Original) The system according to Claim 1, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

7. (Original) The system according to Claim 1, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

8. (Currently Amended) The system according to Claim 1, wherein the means for ~~securely operably connecting~~ establishing a secure, operable connection further comprises means for authenticating the biometric sensor and the card reader to the security component.

9. (Original) The system according to Claim 8, further comprising means for authenticating the security component to the biometric sensor and the card reader.

10. (Currently Amended) The system according to Claim 1, wherein the means for ~~securely operably connecting~~ establishing a secure, operable connection is activated by a hardware reset of the one or more components, and wherein the hardware reset is activated by ~~operably connecting of~~ the established secure, operable connection of the one or more components.

11. (Original) The system according to Claim 8, wherein the means for authenticating the biometric sensor and the card reader are securely stored thereon.

12. (Original) The system according to Claim 8, wherein the means for authenticating further comprises means for using public key cryptography.

13. (Currently Amended) The system according to Claim [[2]]1, further comprising means for concluding that the user is the authorized holder of the card only if the means for comparing succeeds.

14. (Original) The system according to Claim 1, wherein the card is a smart card.

15. (Currently Amended) The system according to Claim [[2]]1, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising means for digitally signing information presented to the card with the private key if the means for comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

16. (Currently Amended) The system according to Claim [[2]]1, wherein the means for comparing is performed by the biometric sensor.

17. (Original) The system according to Claim 16, further comprising means for securely transferring the stored biometric information of the authorized holder to the biometric sensor for use by the means for comparing.

18. (Original) The system according to Claim 17, further comprising means for interrupting the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

19. (Original) The system according to Claim 2, wherein the means for comparing is performed by the security component.

20. (Original) The system according to Claim 15, further comprising means for ~~securely operably connecting~~ establishing a secure, operable connection between an application processing component to and the security component, and wherein the information presented to the card is generated by the established secure, operable ~~securely operably~~ connected application processing component.

21. (Original) The system according to Claim 8, wherein the means for authenticating further comprises means for performing a security handshake between the biometric sensor and the security component and between the card reader and the security component.

22. (Original) The system according to Claim 21, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

23. (Original) The system according to Claim 8, wherein:
the means for authenticating the biometric sensor further comprises means for using (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and

the means for authenticating the card reader further comprises means for using (1) a second unique identifier of the card reader, (2) a second digital signature computed over the second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.

Claims 24-32 (Canceled).

33. (Currently Amended) A computer program product for securely providing biometric input from a user, the computer program product embodied on one or more computer-readable media and comprising:

~~computer-readable program code means for operating configured to operate a biometric sensor;~~

computer-readable program code ~~means for operating~~ configured to operate a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it the security component is securely operably connected;

computer-readable program code configured to operate a biometric sensor that is securely, operably connected, as one of the one or more other components, to the security component;

computer-readable program code ~~means for accessing~~ configured to access a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

computer-readable program code ~~means for operating~~ configured to operate a card reader for repeatedly accessing the stored secrets and stored identifying information, wherein the stored identifying information comprises stored biometric information of the authorized holder and wherein the card reader is configured to repeatedly access the stored secrets and stored identifying information upon beginning a security-sensitive operation and is configured to terminate repeatedly accessing upon completion of the security-sensitive operation;

computer-readable program code ~~means for detecting and responding~~ configured to detect and respond to an operable insertion of the card into the card reader; ~~and~~

computer-readable program code ~~means for securely operably connecting~~ configured to establish a secure, operable connection between the biometric sensor, the card reader, and the security component;

computer readable program code configured to compare the repeatedly obtained biometric information to the stored biometric information of the authorized holder of the card;
and

computer readable program code configured to conclude, within the security component, that the security-sensitive operation is authentic based on all the one or more other components which are securely operably connected to the security component remaining securely operably connected to the security component until completion of the security-sensitive operation.

Claim 34 (Canceled).

35. (Original) The computer program product according to Claim 33, wherein selected ones of the secure operable connections are made using one or more buses of the security component.

36. (Original) The computer program product according to Claim 33, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

37. (Original) The computer program product according to Claim 36, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

38. (Original) The computer program product according to Claim 33, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

39. (Original) The computer program product according to Claim 33, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

40. (Currently Amended) The computer program product according to Claim 33, wherein the computer-readable program code ~~means for securely operably connecting~~ configured to establish a secure, operation connection further comprises computer-readable program code ~~means for authenticating~~ configured to authenticate the biometric sensor and the card reader to the security component.

41. (Currently Amended) The computer program product according to Claim 40, further comprising computer-readable program code ~~means for authenticating~~ configured to authenticate the security component to the biometric sensor and the card reader.

42. (Currently Amended) The computer program product according to Claim 33, wherein the computer-readable program code ~~means for securely operably connecting~~ configured to establish a secure, operable connection is activated by a hardware reset of the one or more components, and wherein the hardware reset is activated by ~~operably connecting of the~~ established secure, operable connection of the one or more components.

43. (Currently Amended) The computer program product according to Claim 40, wherein the computer-readable program code ~~means for authenticating~~ configured to authenticate the biometric sensor and the card reader are securely stored thereon.

44. (Currently Amended) The computer program product according to Claim 40, wherein the computer-readable program code ~~means for authenticating~~ configured to authenticate further comprises computer-readable program code ~~means for using~~ configured to use public key cryptography.

45. (Currently Amended) The computer program product according to Claim ~~[[34]]~~ 33, further comprising computer-readable program code ~~means for concluding~~ configured to conclude that the user is the authorized holder of the card only if the means for comparing succeeds.

46. (Original) The computer program product according to Claim 33, wherein the card is a smart card.

47. (Currently Amended) The computer program product according to Claim [[34]]33, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising computer-readable program code ~~means for digitally signing~~ configured to digitally sign information presented to the card with the private key if the computer-readable program code ~~means for comparing~~ configured to compare succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

48. (Currently Amended) The computer program product according to Claim [[34]]33, wherein the computer-readable program code ~~means for comparing~~ configured to compare is performed by the biometric sensor.

49. (Currently Amended) The computer program product according to Claim 48, further comprising computer-readable program code ~~means for securely transferring~~ configured to securely transfer the stored biometric information of the authorized holder to the biometric sensor for use by the computer-readable program code ~~means for comparing~~ configured to compare.

50. (Currently Amended) The computer program product according to Claim 49, further comprising computer-readable program code ~~means for interrupting~~ configured to interrupt the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

51. (Currently Amended) The computer program product according to Claim [[34]]33, wherein the computer-readable program code ~~means for comparing~~ configured to compare is performed by the security component.

52. (Currently Amended) The computer program product according to Claim 47, further comprising computer- readable program code ~~means for securely operably connecting~~ configured to establish a secure, operable connection between an application processing component ~~to~~ and the security component, and wherein the information presented to the card is generated by the ~~securely operably~~ connected application processing component.

53. (Currently Amended) The computer program product according to Claim 40, wherein the computer-readable program code ~~means for authenticating~~ configured to authenticate further comprises computer-readable program code ~~means for performing~~ configured to perform a security handshake between the biometric sensor and the security component and between the card reader and the security component.

54. (Original) The computer program product according to Claim 53, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

55. (Currently Amended) The computer program product according to Claim 40, wherein:

the computer-readable program code ~~means for authenticating~~ configured to authenticate the biometric sensor further comprises computer-readable program code ~~means for using~~ configured to use (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and

the computer-readable program code ~~means for authenticating~~ configured to authenticate the card reader further comprises computer-readable program code ~~means for using~~ configured to use (1) a second unique identifier of the card reader, (2) a second digital signature computed over

the second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.

56. (Currently Amended) A method of securely providing biometric input from a user, comprising ~~steps of:~~

~~operating a biometric sensor;~~

operating a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it the security component is securely operably connected;

operating a biometric sensor component that is securely, operably connected, as one of the one or more other components, to the security component;

accessing a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

operating a card reader for repeatedly accessing the stored secrets and stored identifying information, wherein the stored identifying information comprises stored biometric information of the authorized holder and wherein the card reader is configured to repeatedly access the stored secrets and stored identifying information upon beginning a security-sensitive operation and is configured to terminate repeatedly accessing upon completion of the security-sensitive operation;

detecting and responding to an operable insertion of the card into the card reader; ~~and~~ securely operably connecting establishing a secure, operable connection the biometric sensor, the card reader, and the security component;

comparing the repeatedly obtained biometric information to the stored biometric information of the authorized holder of the card; and

concluding, within the security component, that the security-sensitive operation is authentic based on all the one or more other components which are securely operably connected to the security component remaining securely operably connected to the security component until completion of the security-sensitive operation.

Claim 57 (Canceled).

58. (Original) The method according to Claim 56, wherein selected ones of the secure operable connections are made using one or more buses of the security component.

59. (Original) The method according to Claim 56, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

60. (Original) The method according to Claim 59, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

61. (Original) The method according to Claim 56, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

62. (Original) The method according to Claim 56, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

63. (Currently Amended) The method according to Claim 56, wherein ~~the step of securely operably connecting~~ establishing a secure, operable connection further comprises the ~~step of~~ authenticating the biometric sensor and the card reader to the security component.

64. (Currently Amended) The method according to Claim 63, further comprising the ~~step of~~ authenticating the security component to the biometric sensor and the card reader.

65. (Currently Amended) The method according to Claim 56, wherein ~~the step of securely operably connecting~~ establishing a secure, operable connection is activated by a hardware reset of the one or more components, and wherein the hardware reset is activated by

~~operably connecting of~~ the established secure, operable connection of the one or more
components.

66. (Original) The method according to Claim 63, wherein instructions for authenticating the biometric sensor and the card reader are securely stored thereon.

67. (Currently Amended) The method according to Claim 63, wherein ~~the step of~~ authenticating further comprises ~~the step of~~ using public key cryptography.

68. (Currently Amended) The method according to Claim ~~[[57]]~~56, further comprising ~~the step of~~ concluding that the user is the authorized holder of the card only if ~~the~~ comparing ~~step~~ succeeds.

69. (Original) The method according to Claim 56, wherein the card is a smart card.

70. (Currently Amended) The method according to Claim ~~[[57]]~~56, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising ~~the step of~~ digitally signing information presented to the card with the private key if ~~the step of~~ comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

71. (Currently Amended) The method according to Claim ~~[[57]]~~56, wherein ~~the step of~~ comparing is performed by the biometric sensor.

72. (Currently Amended) The method according to Claim 71, further comprising ~~the step of~~ securely transferring the stored biometric information of the authorized holder to the biometric sensor for use ~~the step of~~ comparing.

73. (Currently Amended) The method according to Claim 72, further comprising ~~the~~

~~step of~~ interrupting the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

74. (Currently Amended) The method according to Claim ~~[[57]]~~56, wherein ~~the step of~~ comparing is performed by the security component.

75. (Currently Amended) The method according to Claim 70, further comprising ~~the step of securely operably connecting~~ establishing a secure, operable connection an application processing component to the security component,

and wherein the information presented to the card is generated by the securely operably connected application processing component.

76. (Currently Amended) The method according to Claim 63, wherein ~~the step of~~ authenticating further comprises ~~the step of~~ performing a security handshake between the biometric sensor and the security component and between the card reader and the security component.

77. (Original) The method according to Claim 76, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

78. (Currently Amended) The method according to Claim 63, wherein:
~~the step of~~ authenticating the biometric sensor further comprises ~~the step of~~ using (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and

~~the step of~~ authenticating the card reader further comprises ~~the step of~~ using (1) a second

unique identifier of the card reader, (2) a second digital signature computed over the second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.